

# E&CE 710 Topic 4

## Sequence Design and Cryptography, Spring 2009

**Instructor:** Professor G. Gong  
Office: EIT 4158, x35650, ggong@calliope.uwaterloo.ca  
<http://calliope.uwaterloo.ca/~ggong>  
**Time:** 8:30-11:20, Wednesdays  
**Room:** EIT 3151/3152

**Course Description:** This course is an introduction to sequence design and cryptography with applications to communication security. The course covers the basic theory of feedback shift register sequences, randomness criteria, pseudorandom sequence/number generators, correlation attacks, and algebraic attacks. Practical crypto algorithms, stream ciphers, block ciphers, hash functions, MAC, conversion among symmetric key crypto schemes, linear cryptanalysis and differential cryptanalysis. Public-key cryptography, digital signatures, and ID based cryptography. Communication security architecture and infrastructure, certificate authority, mutual authentication, key establishment, network security protocols (IKE, IPsec, TLS), access authentication protocols and infrastructure.

**Prerequisites:** E&CE 150, E&CE 316, or equivalent courses taken from other universities.

### Course Text:

1. S.W. Golomb and G. Gong, *Signal Design for Good Correlation – for Wireless Communication, Cryptography and Radar*, Cambridge University Press, 2005. Chapter 4, and part of Chapters 10 and 11.
2. L.D. Chen and G. Gong, *Communication System Security*, draft, 2008. Chapters 1- 8.
3. Some notes.

### References:

1. D. Stinson, *Cryptography, Theory and Practice*, 3rd ed., CRC Press, 2006. (QA268 S75)
2. C.P. Pfleeger and S.L. Pfleeger, *Security in Computing*, 4th ed., Prentice Hall, 2007. (QA76.9.A25 P45)

**Course Grading:** The course grade will be based on assignments given during the term, one project (a list of project problems will be given, however students are allowed to suggest problems related to their own research), and the final exam.

### Course Outline

1. Introduction to Communication Security: security architecture, basic information security concepts and protection mechanisms, confidentiality, integrity and authenticity, trust model, threat model, trusted platform, and protected communications.

2. Feedback Shift Register (FSR) Sequences: linear FSR (LFSR) sequences, decompositions of LFSRs, randomness measurements, Berlekamp-Massey algorithm and linear complexity, autocorrelation and cross correlation of sequences.
3. Pseudo-random Sequence (Number) Generators: filtering generators, combinatorial function generators, clock-control generators, shrinking generators, Blum-Blum-Shub generators, correlation attacks, and algebraic attacks.
4. Stream Ciphers: one-time-pad, design principles of stream ciphers, practical stream ciphers A5/1, w7, E0, RC4 and RC4-like, stream cipher candidates from ECRYPT (WG, Grain 2 and Trivium), birthday attacks, and time-memory trade-off attacks.
5. Block Ciphers and Hash Functions: design principles of block ciphers, DES and AES, encryption models, secure hash functions, MAC (message authentication code), conversions among symmetric key algorithms, linear cryptanalysis and differential cryptanalysis.
6. Digital Signatures and Identity Based Encryption: security of public-key cryptography, RSA encryption and digital signature, ElGamal digital signature, Digital Signature Standard (DSS), elliptic curve digital signature algorithm (ECDSA), LFSR based DSA, pairing-based IBC, and fault attacks.
7. Security Architecture and Infrastructure: Infrastructure support, authentication server, certificate authority, key generation and distribution.
8. Network Domain Security: the man-in-the-middle attacks, mutual authentication, key establishment, cryptographic algorithm negotiation, protected communications, network security protocols (Internet key exchange and IPsec), and transport layer security (TLS).
9. Access Authentication Protocols and Infrastructure: Basic concepts in access authentication, UMTS and CDMA authentication and key agreement (AKA), authentication, authorization, and accounting (AAA).